UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,696	09/12/2003	David D. Brandt	03AB014C/ALBRP303USC	7375

7590 01/02/2009

Susan M. Donahue
Rockwell Automation, 704-P, IP Department
1201 South 2nd Street
Milwaukee, WI 53204

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
01/02/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/661,696	BRANDT ET AL.	
	Examiner	Art Unit	
	RONALD BAUM	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 October 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,12-17,19-21,23-41 and 45-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *26-29* is/are allowed.

6)☒ Claim(s) *1-9, 12-17, 19-21, 23,30-41 and 45-47* is/are rejected.

7)☒ Claim(s) *24 and 25* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 24 October 2008.

2. Claims 1-9, 12-17, 19-21, 23-41 and 45-47 are pending for examination.

3. Claims 1-9, 12-17, 19-21, 23, 30-41 and 45-47 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-9, 12-17, 19-21, 23, 30-41 and 45-47 are rejected under 35 U.S.C. 102(b) as being anticipated by Swiler et al, U.S. Patent 7,013,395 B1.

Prior Art's Broad Disclosure vs. Preferred Embodiments

As concerning the scope of applicability of cited references used in any art rejections below, as per MPEP § 2123, subsection R.5. Rejection Over Prior Art's Broad Disclosure Instead of Preferred Embodiments:

> I. PATENTS ARE RELEVANT AS PRIOR ART FOR ALL THEY CONTAIN "The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." In re Heck, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re Lemelson, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968)). A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including nonpreferred embodiments. Merck & Co. v. Biocraft Laboratories, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), cert. denied, 493 U.S. 975 (1989). See also > Upsher-Smith Labs. v. Pamlab, LLC, 412 F.3d 1319, 1323, 75 USPQ2d 1213, 1215 (Fed. Cir. 2005)(reference disclosing optional inclusion of a particular component teaches compositions that both do and do not contain that component);< Celeritas Technologies Ltd. v. Rockwell International Corp., 150 F.3d 1354, 1361, 47 USPQ2d 1516, 1522-23 (Fed. Cir. 1998) (The court held that the prior art anticipated the claims even though it taught away from the claimed invention.). >See also MPEP § 2131.05 and § 2145, subsection X.D., which discuss prior art that teaches away from the claimed invention in the context of anticipation and obviousness, respectively.<
>
> II. NONPREFERRED AND ALTERNATIVE EMBODIMENTS CONSTITUTE PRIOR ART
> Disclosed examples and preferred embodiments do not constitute a teaching away from a broader disclosure or nonpreferred embodiments. In re Susi, 440 F.2d 442, 169 USPQ 423 (CCPA 1971). "A known or obvious composition does not become patentable simply because it has been described as somewhat inferior to some other product for the same use." In re Gurley, 27 F.3d 551, 554, 31 USPQ2d 1130, 1132 (Fed. Cir. 1994). Furthermore, "[t]he prior art's mere disclosure of more than one alternative does not constitute a teaching away from any of these alternatives

because such disclosure does not criticize, discredit, or otherwise discourage the solution claimed…." In re Fulton, 391 F.3d 1195, 1201, 73 USPQ2d 1141, 1146 (Fed. Cir. 2004).

Swiler et al *generally* teaches and suggests (i.e., Abstract, figures 1-2 and associated descriptions in general) the limitations set forth in the claims below.

5. As per claim 1; "A security analysis tool for an automation system, comprising:

an interface component that generates

a description of one or more industrial controllers, wherein

the description includes at least one of

shop floor access patterns,

Intranet access patterns,

Internet access patterns, and

wireless access patterns [ABSTRACT, f*igures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., description of* ***factory assets*** *whereas factory automation IT/network elements involved in the operation of a given commercial/industrial/government environment (e.g., col. 1,lines 24-45, col. 5,lines 30-55) encompasses the use of at the very least programmable logic controllers of which industrial controllers are an associated architecture), clearly dealing with Intranet and Internet access patterns insofar as network security per se is concerned) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that*

results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.];

an analyzer component that generates

one or more security outputs

based on the description [*ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information, such that results (i.e., post analysis generated security outputs) used to evaluate (i.e., graphed output information)/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.*];

and

a validation component

that periodically monitors the industrial network controllers

following deployment of the one or more security outputs

to determine one or more vulnerabilities related thereto

[*ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack*

template information, such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, by the operator/user of the computer system analysis tool, such that said attack analysis results are for the utilization on the target system analyzed such that said attacks (i.e., ' vulnerabilities related thereto ') can be prevented/mitigated. The validation aspect applies insofar as the analysis tool clearly is used, at least on a 'periodic basis' forming the basis for the 'following deployment of the one or more security outputs' aspect, clearly encompassing the claimed limitations as broadly interpreted by the examiner.].".

As per claim 12, this claim is the method claim for the system claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

As per claim 16, this claim is the means plus function claim for the system claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

6. Claim 2 ***additionally recites*** the limitation that; "The tool of claim 1,

at least one of

the interface component and

the analyzer component

operate on a computer and

receive

one or more factory inputs

that provide the description.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

7. Claim 3 ***additionally recites*** the limitation that; "The tool of claim 2,

the factory inputs include

user input,

model inputs,

schemas,

formulas,

equations,

files,

maps, and

codes.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component utilizing, at the very least, user input, model inputs, files, maps, and codes) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

8. Claim 4 ***additionally recites*** the limitation that; "The tool of claim 2,

the factory inputs are processed by

the analyzer component to generate the security outputs,

the security outputs including

at least one of

manuals,

documents,

schemas,

executables,

codes,

files,

e-mails,

recommendations,

topologies,

configurations,

application procedures,

parameters,

policies,

rules,

user procedures, and

user practices

that are employed

to facilitate security measures in

an automation system.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information, such that results (i.e., post analysis generated security outputs) used to evaluate (i.e., graphed output information, utilizing, at the very least, topologies, recommendations, files, rules, configurations)/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

9. Claim 5 ***additionally recites*** the limitation that; "The tool of claim 1,

the interface component includes

at least one of

a display output having associated display objects and

at least one input

to facilitate operations with

the analyzer component,

the interface component is associated with

at least one of

an engine,

an application,

an editor tool,

a web browser, and

a web service.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component, utilizing, at the very least, input editing tools, and a display output having associated display objects for the results graphic output) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a

function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

10. Claim 6 ***additionally recites*** the limitation that; "The tool of claim 5,

the display objects include

at least one of

configurable icons,

buttons,

sliders,

input boxes,

selection options,

menus, and

tabs,

the display objects having

multiple configurable

dimensions,

shapes,

colors,

text,

data and

sounds

to facilitate operations with

the analyzer component.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component, utilizing, at the very least, GUI oriented input editing tools, and a display output having associated display objects for the results graphic output) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

11. Claim 7 ***additionally recites*** the limitation that; "The tool of claim 5,

the at least one inputs includes

receiving user commands from

a mouse,

keyboard,

speech input,

web site,

remote web service,

camera, and

video input

to affect operations of

the interface component and

the analyzer component.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component, utilizing, at the very least, GUI oriented input editing tools, and a display output having associated display objects for the results graphic output) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

12. Claim 8 ***additionally recites*** the limitation that; "The tool of claim 1,

the description includes

a model of one or more industrial automation assets

to be protected and

associated network pathways

to access the industrial automation assets.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., description of **factory assets** whereas factory automation IT/network elements involved in the operation of a

given commercial/industrial/government environment (e.g., col. 1,lines 24-45, col. 5,lines 30-55) encompasses the use of at the very least programmable logic controllers of which industrial controllers are an associated architecture) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

13. Claim 9 ***additionally recites*** the limitation that; "The tool of claim 1,

the description

includes at least one of

risk data and

cost data

that is employed by

the analyzer component

to determine suitable security measures.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model, clearly dealing with risk and effective cost insofar as network security per se is concerned) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to

counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

As per claim 13, this claim is the method claim for the system claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection.

14. Claim 14 ***additionally recites*** the limitation that; "The method of claim 12,

the security outputs include at least one of recommended

security components,

codes,

parameters,

settings,

related interconnection topologies,

connection configurations,

application procedures,

security policies,

rules,

user procedures, and

user practices.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system

analysis tool using inputted computer system/network configuration/topology and attack template information, such that results (i.e., post analysis generated security outputs) used to evaluate (i.e., graphed output information, utilizing, at the very least, topologies, recommendations, files, rules, configurations)/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

15. Claim 15 ***additionally recites*** the limitation that; "The method of claim 12, further comprising at least one of:

automatically deploying the security outputs

to one or more entities; and

utilizing the security outputs

to mitigate at least one of

unwanted network access and

network attack.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of

the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

16. As per claim 17; "A security validation system, comprising:

a scanner component

to automatically interrogate an industrial automation device

at periodic intervals for

security related data [*ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.*];

a validation component

to automatically assess security capabilities of the industrial automation device

based upon a comparison of

the security related data and

one or more predetermined security guidelines [*ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities (i.e., a validation component ...) as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.*]; and

a security analysis tool

that recommends interconnection of

one or more industrial automation devices

to achieve a specified security goal [*ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to*

evaluate/make configuration changes (i.e., ' security analysis tool ... recommends interconnection ... a specified security goal ') in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.].".

As per claim 30, this claim is the means plus function claim for the system claim 17 above, and is rejected for the same reasons provided for the claim 17 rejection.

17. Claim 19 ***additionally recites*** the limitation that; "The system of claim 17, the validation component performs at least one of

a security audit,

a vulnerability scan,

a revision check,

an improper configuration check,

file system check,

a registry check,

a database permissions check,

a user privileges check,

a password check, and

an account policy check.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component, insofar as associated with improper configuration, vulnerability, file system check, user privileges check, etc.,), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

18. Claim 20 ***additionally recites*** the limitation that; "The system of claim 17,

the security guidelines

are automatically determined.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

19. Claim 21 ***additionally recites*** the limitation that; "The system of claim 46,

the host-based component performs

vulnerability scanning and

auditing on devices,

the network-based component performs

vulnerability scanning and

auditing on networks.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based/network-based component) analysis tool using inputted (i.e., vulnerability scanner component) computer system/network configuration/topology (i.e., auditing factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

20. Claim 23 ***additionally recites*** the limitation that; "The system of claim 21,

at least one of

host-based component and

the network-based component

at least one of

includes

non-destructively mapping a topology of

IT and

industrial automation devices,

checking revisions and configurations,

checking user attributes, and

checking access control lists.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based/network-based component) analysis tool using inputted (i.e., vulnerability scanner component) computer system/network configuration/topology (i.e., auditing of **factory assets** whereas factory automation IT/network elements involved in the operation of a given commercial/industrial/government environment (e.g., col. 1,lines 24-45, col. 5,lines 30-55) encompasses the use of at the very least programmable logic controllers of which industrial controllers are an associated architecture) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

21. As per claim 31; "A security learning system for an industrial automation environment, comprising:

a learning component

to monitor and learn industrial automation activities during

a training period [*ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool (i.e., learning/ monitoring/scanning component) using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning of automation activities) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.*];

and

a detection component

to automatically trigger a security event based upon

detected deviations of subsequent industrial automation activities

after the training period [*ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning) and gathering associated data such as IP address, machine type, operating system, file system*

structure, etc.,) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities (i.e., a detection component ... trigger a security event ... after the training period) as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.].".

As per claim 39, this claim is the method claim for the system claim 31 above, and is rejected for the same reasons provided for the claim 31 rejection.

As per claim 41, this claim is the means plus function claim for the system claim 31 above, and is rejected for the same reasons provided for the claim 31 rejection.

22. Claim 32 ***additionally recites*** the limitation that; "The system of claim 31,

the industrial automation activities includes at least one of

a network activity and

a device activity.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based device activity /network-based activity component) analysis tool using inputted (i.e., scanner automation activities component) computer system/network configuration/topology

and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

23. Claim 33 ***additionally recites*** the limitation that; "The system of claim 31,

the learning component including

at least one of

a learning model and

a variable.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool (i.e., learning/ monitoring/scanning component) using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning of automation activities) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., learning model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

24. Claim 34 ***additionally recites*** the limitation that; "The system of claim 31,

the industrial automation activities include

at least one of

a number of network requests,

a type of network requests,

a time of requests,

a location of requests,

status information, and

counter data.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool (i.e., learning/ monitoring/scanning component) using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning of automation activities, such as number of network requests, type of network requests, location of requests, etc.,) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., learning model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

25. Claim 35 ***additionally recites*** the limitation that; "The system of claim 31,

the detection component employs

at least one of

a threshold and

a range to determine the deviations.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool (i.e., learning detection/monitoring/scanning component) using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning of automation activities, such as number of network requests, type of network requests, location of requests, etc.,) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., learning model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

26. Claim 36 ***additionally recites*** the limitation that; "The system of claim 35,

the threshold and

the range

are dynamically adjustable.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system

analysis tool (i.e., learning detection/monitoring/scanning component) using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning of automation activities, such as number of network requests, type of network requests, location of requests, etc.,) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., learning model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

27. Claim 37 ***additionally recites*** the limitation that; "The system of claim 33,

the learning model includes

at least one of

mathematical models,

statistical models,

probabilistic models,

functions,

algorithms, and

neural networks,

classifiers,

inference models,

Hidden Markov Models (HMM),

Bayesian models,

Support Vector Machines (SVM),

vector-based models, and

decision trees.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool (i.e., learning/ monitoring/scanning component) using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning of automation activities) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., learning model) information dealing with hypothesized (i.e., mathematical, statistical, probabilistic models, etc.,) attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

28. Claim 38 ***additionally recites*** the limitation that; "The system of claim 31,

the security event includes

at least one of

automatically performing corrective actions,

altering network patterns,

adding security components,

removing security components,

adjusting security parameters,

firing an alarm, notifying an entity,

generating an e-mail,

interacting with a web site, and

generating security data

to mitigate network security problems.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities (i.e., security event … altering network patterns … adjusting security parameters, generating security data, etc.,) as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

29. Claim 40 ***additionally recites*** the limitation that; "The method of claim 39,

the at least one data pattern

employed as input for

a security analysis process.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool (i.e., learning/ monitoring/scanning component) using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning of automation activities) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., learning model) information dealing with hypothesized (i.e., mathematical, statistical, probabilistic models, etc.,) attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

30. Claim 45 ***additionally recites*** the limitation that; "The tool of claim 1,

the analyzer component is adapted for

partitioned security specification entry and

sign-off from various groups.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., the network partitioned security specification) and attack template (i.e., inclusive of authentication aspects, insofar as sign-on/sign-off, at the very least would be concerned) information dealing with

hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

31. Claim 46 ***additionally recites*** the limitation that; "The system of claim 17,

the scanner component and

the validation component

are at least one of

a host-based component and

a network-based component.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based/network-based component) analysis tool using inputted (i.e., scanner component) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

32. Claim 47 ***additionally recites*** the limitation that; "The system of claim 21,

at least one of

host-based component and

the network-based component

at least one of

determines susceptibility to

common network-based attacks,

searches for

open TCP/UDP ports,

scans for

vulnerable network services,

attempts to gain identity information about

end devices that relates to

hacker entry,

performs vulnerability

scanning and

auditing

on

firewalls,

routers,

security devices, and

factory protocols.”.

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based/network-based component) analysis tool using inputted (i.e., vulnerability scanner component) computer system/network configuration/topology (i.e., auditing factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

Response to Amendment

33. As per applicant's argument concerning the lack of teaching by Swiler et al of the validation component periodic monitoring following deployment embodiment aspects, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive.

At the very least, as detailed in the claim 1 rejection above, the Swiler et al teachings of the validation aspect applying insofar as the analysis tool clearly is used, at least on a 'periodic basis' forming the basis for the 'following deployment of the one or more security outputs' aspect per se, as broadly interpreted by the examiner, and would therefore be applicable in the rejection, such that the rejection support references collectively encompass the said claim limitations in their entirety.

34. As per applicant's argument concerning the lack of teaching by Swiler et al of the 'industrial controller' embodiment aspects, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive.

At the very least, as detailed in the claim 1 rejection above, and the previous office action rejection, the Swiler et al teachings of aspects of factory assets, whereas factory automation IT/network elements involved in the operation of a given commercial/industrial/government environment (e.g., col. 1,lines 24-45, col. 5,lines 30-55) encompasses the use of at the very least programmable logic controllers of which industrial controllers are an associated architecture aspect, and generally industrial controller factory assets per se, as *broadly interpreted by the examiner*, and would therefore be applicable in the rejection, such that the rejection support references collectively encompass the said claim limitations in their entirety.

35. As per applicant's argument concerning the lack of teaching by Swiler et al of the learning/applying aspect of the deviation of pattern detection, and automated remediation of same, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive.

At the very least, as detailed above, the ***user*** of the analysis tool (i.e., ' means …') will certainly apply results obtained of potential/detected attack/vulnerabilities so as to mitigate said attack/vulnerabilities via the system (i.e., automated as per by any reasonable definition of an automated system), and, deviation, threshold and out of tolerance detection aspects are clearly encompassed via the state detection (e.g., 'edge' state analysis aspects and associated reported results), resulting in an effective notification of the user (i.e., 'generating an alarm') of

attack/vulnerabilities, as *broadly interpreted by the examiner*, and would therefore be applicable in the rejection, such that the rejection support references collectively encompass the said claim limitations in their entirety.

36. As per applicant's argument concerning the lack of teaching by Swiler et al of the 'initiated security procedure …' aspect of the claim, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive.

The limitation does not add patentable distinction beyond the aspects of the claim as they are presently rejected, as *broadly interpreted by the examiner*, and would therefore be applicable in the rejection, such that the rejection support references collectively encompass the said claim limitations in their entirety.

Allowable Subject Matter

37. Claims 24 and 25 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

38. Claims 26-29 are allowed.

39. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

40. The examiner suggests for the sake of moving prosecution forward that the applicant direct the amendment of claim limitations towards qualifying more explicitly the ' automated ' aspects of various components, insofar as those specifics that differentiate the inventive concept from embodiments that merely allow for a user utilizing an ' automated ' device/processing element, generally involved in the reference, and possible related art.

41. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand, can be reached at (571) 272-3811. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

/R. B./

Examiner, Art Unit 2439

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434